Extreme Flow Optimizer

CERN openlab Technical Workshop 2019

Stefan.Stancu@cern.ch
Project fellow: Adam Krajewski

24/01/2019
Project overview (1)

• Initially collaboration between CERN and Brocade
  • Started in June 2015 as a 2-year project
  • Fellow recruited and strongly integrated with Brocade’s software development team
  • Initial goal:
    • Get expertise in the Brocade Flow Optimizer (BFO), a Software Defined Networking application
    • Enhance and generalize the BFO software architecture

• Evolution of goals:
  • Adapt BFO to build an intelligent network traffic steering system answering CERN’s needs
    • Define use cases and requirements for them:
      • Intrusion Detection System (IDS) automation
      • Firewall load-balancing
      • Advanced policy-based routing engine
    • Implement necessary features
  • Enhance BFO software architecture

Extreme Flow optimizer -- stefan.stancu@cern.ch
Project overview (2)

• Project continuation
  • Brocade acquired by Broadcom; Data Center BU acquired by Extreme Networks
  • Successful project handover and extension for the 3rd year
  • **Brocade** Flow Optimizer becomes **Extreme** Flow Optimizer (EFO)

• Final goals:
  • **Primary focus on the Intrusion Detection System use case**
  • Switch SDN focus from OpenFlow to more generic network automation
    • Programmatically leverage proprietary hardware features through open-source platforms
    • Use StackStorm / Extreme Workflow Composer
  • Continue capitalizing on the acquired expertise
    • Further contributions to commercial software development
Extreme Flow Optimizer (EFO)

- Software Defined Networking application

- Monitoring large traffic flows and organizing them in a controlled manner
  - Traffic visibility through sFlow
  - Dynamic flow management through OpenFlow or CLI
    - Dropping, redirecting, mirroring, metering… and much more!
  - REST API for northbound integrations
    - Bro plugin developed within the openlab collaboration

- Integration with StackStorm
StackStorm / EWC

Extreme Workflow Composer

- Platform for integration and automation across IT services and tools
  - Python-based & open-source
  - https://stackstorm.com/

- Trigger-based workflow execution
  - Sensors listening to events (e.g. syslog)
  - Events translated to Triggers
  - Rules matching Triggers to Actions
  - Workflows grouping Actions together

- Enterprise edition: Extreme Workflow Composer (EWC)
Product contributions

• Nearly 3 years of regular software development effort
  • Full-stack (frontend + backend) developer
  • Reporting to technical managers and product managers
  • Providing occasional technical expertise for customers in Switzerland

• Commercial feature ownerships (design, development, SQA):
  • Bro Integration
  • Palo Alto Networks Integration
  • Arbitrary Bitmask Support for IPv4
  • IP Blacklisting

• Strategic feature involvement:
  • Application tuning for better scalability
  • StackStorm orchestration for Docker

Extreme Flow optimizer -- stefan.stancu@cern.ch
IDS at CERN

• The volume of traffic entering and leaving CERN is growing continuously

• Precise traffic analysis and monitoring is crucial for network security
  • Cyber security threats can be detected and mitigated

• Built a scalable and extensible IDS system at CERN

• Design:
  • Mirror traffic at network boundaries
  • Aggregate and load-balance the traffic across a set of servers
  • Advanced features, enabled by EWC and EFO
    • Symmetrical load-balancing
    • Traffic shunting
IDS setup

Network Automation

EWC

EFO

EFO-Bro integration (plugin)

Configure

Monitor

Aggregate mirrored traffic

SLX 9540

Load balance

Servers running Bro

Scientific Networks

CERN Campus Network

Public Internet

LHC Network

CERN openlab

Extreme Flow optimizer -- stefan.stancu@cern.ch
Project end and outcome

The project ended in October 2018

• Numerous EFO software enhancements done by openlab fellow
• Ultimate result: upgraded, scalable IDS system for CERN
  • In production since the end of 2018
  • Relies on a traffic orchestrator leveraging Extreme Networks technology
    • Hardware: SLX family
    • Software: EFO and EWO platforms

• Yet another successful example of how openlab enables win-win collaborations between CERN and industry partners.
Extreme Flow Optimizer

Questions?

Stefan.Stancu@cern.ch
Project fellow: Adam Krajewski

24/01/2019